PATENT ABSTRACTS OF JAPAN

(11)Publication number : 01-212041
(43)Date of publication of application : 25.08.1989

(51)Int.Cl. H04L 9/02

(21)Application number : 63-036717
(22)Date of filing : 18.02.1988

(71)Applicant : HITACHI LTD
(72)Inventor : HAYASHI KENJI
EBINA OSAMU

(54) CRYPTOGRAPHIC COMMUNICATION SYSTEM

(57)Abstract:
PURPOSE: To enhance the safety of the system by using time series information in common to the system so as to revise ciphering and deciphering algorithm at the transmission side and the reception side thereby applying cryptographic communication.
CONSTITUTION: In case of the transmission by the system, a selection command means uses time series information in common from a time series information generating means to select and command a ciphering algorithm and a cryptographic key used by a ciphering processing means. In case of the reception by the system, the selection command means uses time series information in common from the time series information generating means to select and command a decoding algorithm and a decoding key used by a deciphering processing means. Since the ciphering processing and the deciphering processing are applied by using the conversion algorithm revised in response to the time of communication and the key revised in response to time, then the safety is enhanced.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　平1－212041

⑤1Int.Cl.⁴　識別記号　庁内整理番号　⑬公開　平成1年(1989)8月25日
H 04 L 9/02　Z－7240－5K

審査請求　未請求　請求項の数 1　（全8頁）

⑤4発明の名称　暗号化通信システム

⑳特　願　昭63－36717
㉒出　願　昭63(1988)2月18日

⑦2発明者　林　謙治　神奈川県秦野市堀山下1番地　株式会社日立製作所神奈川工場内
⑦2発明者　海老名　修　神奈川県秦野市堀山下1番地　株式会社日立製作所神奈川工場内
⑦1出願人　株式会社日立製作所　東京都千代田区神田駿河台4丁目6番地
⑦4代理人　弁理士　秋田　収喜

明細書

1．発明の名称

暗号化通信システム

2．特許請求の範囲

1．複数のシステム間で機密保護を要する情報の通信を行う通信システムにおいて、通信システムに共通の時系列情報を生成する時系列情報生成手段を設け、各システムには、複数の暗号化アルゴリズムおよび複数の暗号鍵を備えた暗号化処理手段と、複数の復号化アルゴリズムおよび複数の復号鍵を備えた復号化処理手段と、前記時系列情報により前記暗号化処理手段で用いる暗号化アルゴリズムおよび暗号鍵を選択指示し、前記時系列情報により前記復号化処理手段で用いる復号化アルゴリズムおよび復号鍵を選択指示する選択指示手段とを有することを特徴とする暗号化通信システム。

3．発明の詳細な説明

〔産業上の利用分野〕

本発明は、暗号化通信システムに関し、特に、複数システム間で機密保護を要する情報の通信を行うシステムにおける暗号化通信システムに関するものである。

〔従来の技術〕

従来、機密保護通信を行うための暗号化技術として、米国の標準暗号化方式（ＤＥＳ）等が知られている。この暗号化技術の詳細は、例えば、日経エレクトロニクス，1978年9月4日号，第68頁～第103頁，「鍵なしではまず解けなくなった最近の暗号方式」に記載されている。また、他の暗号化方式に関する技術として、例えば、特開昭６０－１７１５８３号公報に記載されているような、暗号化キーを乱数により生成するものが知られている。

〔発明が解決しようとする課題〕

ところで、暗号化方式においては、鍵（暗号鍵または解読鍵）情報と変換アルゴリズム（暗号化アルゴリズムまたは復号化アルゴリズム）情報がわかれば、一般的に、暗号文の解読が可能である。そのため、管理不備，不注意等により、鍵情報および変換アルゴリズム情報が盗用されると、通信

の機密を守ることは困難となる。このため、例えば、特開昭60－171583号公報に示されるように、暗号化キーを固定的なものとせず、乱数に応じて暗号化キーを生成して、暗号化出力を変えるような方式とするものがあるが、このような方式においては、乱数機構を必要とするため構成が複雑になると共に、暗号化通信を行うシステム間では、送信側および受信側における暗号化キーおよび復号化キーを対応付けて、どのような鍵で暗号化を行うかを管理するための制御が複雑となるという問題があった。

機密保護を要する情報の通信を行うシステム間の通信システムとして、例えば、遠隔に設置されたATM(Automatic Teller Machine)とホスト計算機とが通信回線により接続されて、通信を行うシステムがある。このシステムにおいて、ATM機で現金受授の取引処理を行う場合、ユーザは機密情報である暗証番号のパスワードをATM機に入力する。ユーザが入力したパスワードは暗号化されて、通信回線を通して送信される。このとき、入力したパスワードを暗号化したデータが回線上またはATM機において傍受された場合には、例えば、暗号解読を行わなくても、暗号文そのもののコピーを通信回線上に何らかの手段を使って流すことにより、不正使用される可能性がある。すなわち、暗号文そのものが盗用されることに対しては、固定の変換アルゴリズムと固定の鍵による暗号化では不正使用を防ぐことができないという問題があった。

本発明の目的は、暗号文そのものの盗用に対しても安全度が高い暗号化通信システムを提供することにある。

本発明の前記ならびにその他の目的と新規な特徴は、本明細書の記述及び添付図面によって明らかになるであろう。

〔課題を解決するための手段〕

上記目的を達成するため、本発明においては、複数のシステム間で機密保護を要する情報の通信を行う通信システムにおいて、通信システムに共通の時系列情報を生成する時系列情報生成手段を設け、各システムには、複数の暗号化アルゴリズムおよび複数の暗号鍵を備えた暗号化処理手段と、複数の復号化アルゴリズムおよび複数の復号鍵を備えた復号化処理手段と、前記時系列情報により前記暗号化処理手段で用いる暗号化アルゴリズムおよび暗号鍵を選択指示し、前記時系列情報により前記復号化処理手段で用いる復号化アルゴリズムおよび復号鍵を選択指示する選択指示手段とを有することを特徴とする。

〔作用〕

前記手段によれば、通信システムに共通の時系列情報を生成する時系列情報生成手段が設けられる。また、通信を行う各システムには、複数の暗号化アルゴリズムおよび複数の暗号鍵を備えた暗号化処理手段と、複数の復号化アルゴリズムおよび複数の復号鍵を備えた復号化処理手段と、選択指示手段が設けられる。選択指示手段は、システムが送信を行う場合、時系列情報生成手段からの共通の時系列情報により暗号化処理手段で用いる暗号化アルゴリズムおよび暗号鍵を選択指示する。また、システムが受信を行う場合、時系列情報生成手段からの共通の時系列情報により復号化処理手段で用いる復号化アルゴリズムおよび復号鍵を選択指示する。

すなわち、この通信システムでは、時間情報または計数情報等のシステムに共通の時系列情報により、通信データの送信側システムが、複数の暗号化アルゴリズムと複数の暗号鍵の中から使用する暗号化アルゴリズムと暗号鍵を選択して、暗号化処理手段で通信データの暗号化を行い、通信データを送出する。また、通信データの受信側システムでは、送信側システムと同じ共通の時系列情報によって、複数の復号化アルゴリズムと複数の復号鍵の中から、送信側システムで選択されている暗号化アルゴリズムと暗号鍵に対応した復号化アルゴリズムと復号鍵を選択して、復号化処理手段により、受信した通信データの復号を行う。

このように、暗号化処理および復号化処理は、通信を行う時間に応じて変更される変換アルゴリズムと、時間に応じて変更される鍵を使用して行

われるため、通信を行うシステムの間で保有する暗号化アルゴリズムと暗号鍵の一部の情報が、不正にデータを入手しようとする者に知られても、何時、どのように変換アルゴリズムと鍵とが組合わされて暗号化に使用するのかと知られていなければ、暗号が解読されず、安全性が高められる。また、仮に一部のデータの暗号が解読されても、変更された未知の暗号化アルゴリズムと暗号鍵とで暗号化したデータは解読されることはない。更に、全ての変換アルゴリズム情報と全ての鍵情報が知られても、入手した暗号文にどの変換アルゴリズムと鍵の組み合せが用いているかがわからなければ、暗号解読にはかなりの時間がかかる。このため、安全度はかなり高いものとなる。

時間帯により暗号化に使用する変換アルゴリズムと暗号鍵が異なるようにしているので、不正使用者が暗号文のコピーを回線上に流しても、特定の暗号文の有効時間が制限されているため、暗号文そのものの盗用に対する不正を排除することができる。

〔実施例〕

以下、本発明の一実施例を図面を用いて具体的に説明する。

第１図は、本発明の一実施例にかかる暗号化通信システムの暗号通信機構の要部の構成を示すブロック図である。第１図において、10は送信側システムとなるＡＴＭ機等の端末機、11は共通の時系列情報を発生する時計機構、12は番地生成回路である。13はテーブルメモリであり、複数の暗号化アルゴリズム情報と複数の暗号鍵が記憶されている。14は処理用メモリ、15は暗号化処理を行う処理装置、16は送信データが保持されている送信データ保持部である。また、20は受信側システムとなるホスト計算機、22は番地生成回路である。23はテーブルメモリであり、複数の復号化アルゴリズム情報と複数の復号鍵が記憶されている。24は処理用メモリ、25は復号化処理を行う処理装置、26は復号した受信データを保持する受信データ保持部である。30は通信回線であり、通信回線30により端末機10とホスト計算機20が結合されて、通信システムが構成されている。

第１図に示す通信システムにおいては、通信システムの共通の時系列情報を発生する時計機構11が設けられている。時計機構11から発生する時刻情報は、送信側の番地生成回路12に与えられると共に、通信回線30を介して受信側の番地生成回路22に与えられる。送信側の番地生成回路12は時刻情報を受けると、時刻情報に対応して選択すべき暗号化アルゴリズムと暗号鍵を指示するため、予め時刻情報に対応して設定されているテーブルメモリ13のアドレス情報を発生して、テーブルメモリ13に供給する。テーブルメモリ13では番地生成回路12から供給されたアドレス情報により、テーブルメモリ13に格納されている複数の暗号化アルゴリズムと複数の暗号鍵の中から１つを選択して読出し、使用する暗号化アルゴリズムと暗号鍵を処理装置15に与える。これにより、処理装置15はテーブルメモリ13から選択されて供給された暗号化アルゴリズムと暗号鍵を処理用メモリ14に格納するので、選択された暗号化アルゴリズムと暗号鍵により暗号化処理が行えるようになる。一方、処理装置15には送信データ保持部16から送信すべき送信データが供給されており、処理装置15は、処理用メモリ14を用いて処理に必要なデータの記憶などを行い、送信データの暗号化処理を行う。そして、処理装置15は暗号化した送信データを、通信回線30を介して、受信側システムのホスト計算機20に送信する。

一方、受信側システムのホスト計算機20においては、システム共通の時計機構11からの時刻情報が、通信回線30を介して受信側の番地生成回路22に与えられると、受信側の番地生成回路22は、当該時刻情報を受けて、時刻情報に対応して選択すべき復号化アルゴリズムと復号鍵（送信側システムで選択される暗号化アルゴリズムと暗号鍵に対応している）を指示するため、予め時間帯情報に対応して設定されているテーブルメモリ23のアドレス情報を発生して、テーブルメモリ23に供給する。テーブルメモリ23では番地生成回路22から供給されたアドレス情報により、テーブルメモリ23

に格納されている複数の復号化アルゴリズムと複数の復号鍵の中から１つを選択して読出し、使用する復号化アルゴリズムと復号鍵を処理装置15に与える。これにより、処理装置25はテーブルメモリ28から選択されて供給された復号化アルゴリズムと復号鍵を処理用メモリ24に格納するので、選択された復号化アルゴリズムと復号鍵により暗号データの復号処理が行えるようになる。

一方、処理装置25には、送信側システムから通信回線30を介して送信された暗号化したデータが受信されて供給されており、処理装置25は、処理用メモリ24に格納された復号化アルゴリズムと復号鍵にしたがい、暗号化したデータの復号処理を行う。そして、処理装置25により復号化された受信データは、受信データ保持部26に供給され、保持される。

第２図は、第１図の暗号化通信システムにおける暗号化通信の処理動作を具体的に示すブロック図である。また、第３図は、送信側システムおよび受信側システムにおける暗号化処理および復号化処理の動作を示すフローチャートである。

まず、第２図を参照して、暗号化処理および復号化処理の処理動作において用いられるテーブルデータの構成を説明する。送信側システムの端末機10においては、番地生成回路12が与えられた時刻情報からテーブル方式でアドレスを生成するため、番地生成回路12には時間帯情報2a，暗号化アルゴリズムアドレス2b，暗号鍵アドレス2cをテーブルデータとして格納した番地生成テーブル２が備えられている。また、テーブルメモリ13には、暗号化アルゴリズムアドレス3aに対応させて暗号化アルゴリズム3bを格納し、複数の暗号化アルゴリズムをテーブルデータとして格納している暗号化アルゴリズムテーブル３と、暗号鍵アドレス4aに対応させて暗号鍵4bを格納し、複数の暗号鍵をテーブルデータとして格納している暗号鍵テーブル４とが設けられている。

一方、受信側システムのホスト計算機20においても同様に、番地生成回路22が与えられた時刻情報からテーブル方式でアドレスを生成するため、番地生成回路22には時間帯情報7a，復号化アルゴリズムアドレス7b，復号鍵アドレス7cをテーブルデータとして格納した番地生成テーブル７が備えられている。また、テーブルメモリ23には、復号化アルゴリズムアドレス8aに対応させて復号化アルゴリズム8bを格納し、複数の復号化アルゴリズムをテーブルデータとして格納している復号化アルゴリズムテーブル８と、復号鍵アドレス9aに対応させて復号鍵9bを格納し、複数の復号鍵をテーブルデータとして格納している復号鍵テーブル９とが設けられている。

第３図において、左側のフローチャートは、送信側システムの暗号化処理の動作を示すフローチャートである。また、右側のフローチャートは、受信側システムの復号化処理の動作を示すフローチャートである。

第２図を参照しつつ、第３図のフローチャートにより処理動作を説明する。暗号化処理を行う送信側システムの端末機では、まず、送信要求が端末側に発生したとき、ステップ５１において、時計機構11から、その時の時刻である例えば９時３０分の時刻情報（Ｔ＝９：３０）を番地生成テーブル２に送出すると共に、当該時刻情報を受信システムのホスト計算機側に転送する。なお、このとき、ホスト計算機側に転送する時刻情報は、この時まで使用されている変換アルゴリズムと鍵を保持している暗号化処理部５と復号化処理部６とを介して、通信回線上を暗号文の形式で転送する。次にステップ５２において、与えられた時刻情報から番地生成テーブル２で時間帯情報2aを参照して、当該時刻情報が入る時間帯から暗号化アルゴリズムアドレス2bのアルゴリズムアドレス②と、暗号鍵アドレス2cの鍵アドレス①とを読出す。すなわち、番地生成テーブル２において時刻情報Ｔ＝９：３０を参照キーとして時間帯情報2aの参照を行い、当該する時間帯の欄から暗号化アルゴリズムテーブル３に対するアルゴリズムアドレス②と暗号鍵テーブル４に対する鍵アドレス①とを読出す。次にステップ５３で、得られたアルゴリズムアドレス②を参照キーとして暗号化アルゴリズ

ムテーブル３から、暗号化アルゴリズム3bのアルゴリズムｂを読出す。続いてステップ５４で、得られた鍵アドレス①を参照キーとして暗号鍵テーブル４から、暗号鍵4bの鍵Ａを読出す。次にステップ５５において、読出した暗号化アルゴリズムｂと鍵Ａとを暗号化処理部５に供給する。これにより、暗号化処理部５では暗号化アルゴリズムｂと鍵Ａにより、暗号化プログラムが設定され、機密通信を行うための暗号化処理の準備が完了する。次に、ステップ５６において、送信データ保持部16から送信データを暗号化処理部５に送り、送信データを暗号化して通信回線を介して送信する。このようにして暗号化通信を開始する。

一方、復号化処理を行う受信側システムのホスト計算機では、ステップ６１において、端末機から送信されてきた時刻情報を受信し、この時刻情報（Ｔ＝９：３０）を番地生成テーブル７に送出する。次にステップ６２において、与えられた時刻情報を参照キーとして番地生成テーブル７で時間帯情報7aを参照して、当該時刻情報が入る時間帯から復号化アルゴリズムアドレス7bのアルゴリズムアドレス②と、復号鍵アドレス7cの鍵アドレス①とを読出す。次にステップ６３で、得られたアルゴリズムアドレス②を参照キーとして復号化アルゴリズムテーブル８から、復号化アルゴリズム8bのアルゴリズムｂ′を読出す。続いてステップ６４で、得られた鍵アドレス①を参照キーとして復号鍵テーブル９から、復号鍵9bの鍵Ａ′を読出す。次にステップ６５において、読出した復号化アルゴリズムｂ′と鍵Ａ′とを復号化処理部６に供給する。これにより、復号化処理部６では暗号化アルゴリズムｂ′と鍵Ａ′により、復号化プログラムが設定され、機密通信を行うための復号化処理の準備が完了する。次にステップ６６において、端末機から暗号化したデータを受信し、復号化処理部６で復号化処理を行い、暗号文データからの平文データとしたデータを受信データ保持部26に出力する。

次に、このような実施例における変形例を説明する。上述した実施例によれば、暗号化処理部の暗号化処理および復号化処理部の復号化処理は、それぞれ変換アルゴリズムと鍵を用いるものとしているが、鍵を必要としない変換アルゴリズムを用いるようにしても良い。この場合には、変換アルゴリズムのみを複数種用意している変換アルゴリズムテーブルを備え、時系列情報による選択指示により、変換アルゴリズムのみの選択を行い、選択された変換アルゴリズムで暗号化処理および復号化処理を行い、暗号文の通信を行う。

また、上述した実施例において、暗号化処理部および復号化処理部における変換アルゴリズムと鍵とを変更するタイミングとしての番地生成テーブル２を参照するタイミングは、端末機において通信要求が生じ、時計機構のタイムスタンプが行われた時点としているが、例えば、通信セッション毎，テキスト毎，一定時間間隔毎などのタイミングとしても良い。

また、暗号化処理および復号化処理の処理動作において用いられるテーブルデータを格納しているテーブルは、全て書き換え可能なメモリ（ＲＡＭ：Random Access Memory)で構成し、端末機10の各テーブルデータは、ホスト計算機20からのオンラインロードにより、またはホスト計算機20で作成したフロッピーディスクなどのメディアの配送により、テーブルデータの内容を容換えられるようにしても良い。これにより、使用する変換アルゴリズムと鍵の種類を更に広範囲に可変することができるので、機密通信の安全度は更に高くなる。また、ホスト計算機内に変換アルゴリズムと鍵のデータベースを持てば、その可能な組み合わせは更に大きなものにできるので、機密通信の安全度は非常に高くなる。

また、上述の実施例の説明において、暗号化通信は端末機10からホスト計算機20への一方向の通信のみを示しているが、双方向通信の場合には、端末機10に復号化処理部を備え、ホスト計算機20には暗号化処理部を備えることより、同様にして双方向で暗号化通信を行うことができる。

また、本実施例では、時計機構11として時計そのものを用いているが、これはカウンタなど計数

機能，時計機能等の時系列情報を発生させるものであれば、どのようなものを用いても良い。また、番地生成回路12，22はテーブル参照方式としているが、これに限らず、例えば関数演算により、所定のアドレスを生成するような回路手段を用いるようにしても良い。

更に、また、時計機構11は端末機10側ではなく、ホスト計算機20側に設けるようにしても良い。この時計機構11は、システムに共通の時系列情報を発生するものであれば良いので、どこに設置しても良く、例えば、ホスト計算機の時計機構を用いるようにして、ホスト計算機に接続される全ての端末機の時刻情報は、ホスト計算機の時計機構のタイムスタンプによるものとしても良い。

上述した本実施例の暗号化通信システムを運用する場合、例えば、番地生成テーブルを毎日、あるいは一定期間毎に書き換え、毎日同時間帯に同一の変換アルゴリズムと鍵を使われないようにすれば、システムの安全度を更に高くすることができる。但し、この場合、機密通信を行うシステム間で必要なテーブルデータの設定を済ませ、何時から更新後のテーブルデータの内容により通信をを行うかを予め決めておく必要がある。

第４図は、この暗号化通信システムを運用するための番地生成テーブルの一例を示す図である。第４図に示すように、番地生成テーブル２は、センタ（ホスト計算機）で既に定まっている１日の業務予定40にしたがって、対応付けを行い作成される。このような番地生成テーブルを作成することより、１日あるいは一定期間のある時間帯に適切な暗号化処理を行うようにできる。例えば、第４図において、システムセットアップ時間である８：００～８：３０の間は、ホスト計算機と端末機の間でシステムセットアップ情報の交換のデータ転送を行う時間なので、機密情報の転送は行わない。このため、暗号化処理を行わず、このための変換アルゴリズムおよび鍵の設定を行わない。次の時間帯の８：３１～９：００の間は前日の売上情報を転送する時間帯なので、ある程度解読しにくい暗号化処理を行うため、変換アルゴリズムとしてはアルゴリズムａを、鍵としては鍵Ａを設定する。次の時間帯の９：０１～１２：００の間は顧客の情報を転送する時間帯なので、非常に解読困難な暗号化処理を行うように、変換アルゴリズムとしてはアルゴリズムｂを、鍵としては鍵Ｂを設定する。同様にして、各時間帯に対してそれぞれに変換アルゴリズムおよび鍵を設定して、番地生成テーブルを作成する。このようにして作成した番地生成テーブルより暗号化通信システムを運用することより、柔軟な機密通信の運用を行うことができる。

以上、本発明を実施例にもとづき具体的に説明したが、本発明は、前記実施例に限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能であることは言うまでもない。

〔発明の効果〕

以上、説明したように、本発明の暗号化通信システムによれば、システムに共通の時系列情報により、送信側および受信側で暗号化および復号化アルゴリズムを変更して、暗号化通信を行うので、システムの安全度が高くなり、具体的には次のような効果がある。

（１）複数の鍵および複数の変換アルゴリズムを用いるので、暗号鍵および暗号化アルゴリズムの情報の一部が盗まれても、何時、どの暗号鍵とどの暗号化アルゴリズムを使って暗号化を行うのかという情報がわからなければ、不正に入手した暗号文の暗号の解読を行うことはできず、システムの安全性が高くなる。

（２）たとえ、全ての暗号化アルゴリズム情報と全ての暗号鍵情報がわかっても、入手した暗号文の解読には、全ての暗号化アルゴリズムと全ての暗号鍵の組合せを試めさなければならないので、暗号解読には非常に多くの時間がかかる。このため、システムの安全性が高くなる。

（３）時間帯により暗号化に使用する変換アルゴリズムと暗号鍵を変えるので、一定のデータの暗号化処理結果が常に同一とはならず、暗号文そのものの盗用による不正を防ぐことができる。

４．図面の簡単な説明

第１図は、本発明の一実施例にかかる暗号化通信システムの暗号通信機構の要部の構成を示すブロック図、

第２図は、第１図の暗号化通信システムにおける暗号化通信の処理動作を示すブロック図、

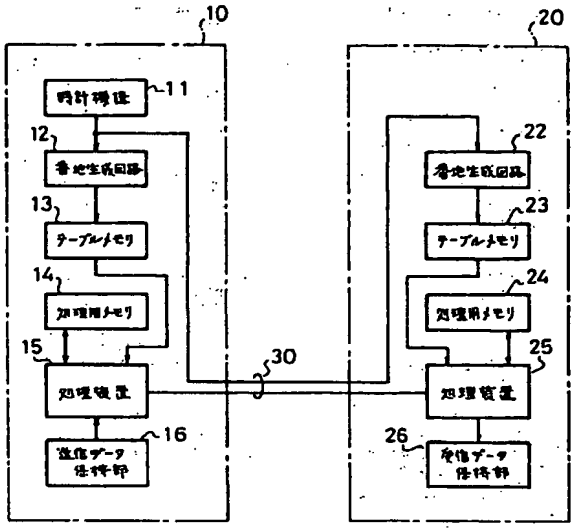
第３図は、送信側システムおよび受信側システムにおける暗号化処理および復号化処理の動作を示すフローチャート、

第４図は、暗号化通信システムを運用するための番地生成テーブルの一例を示す図である。

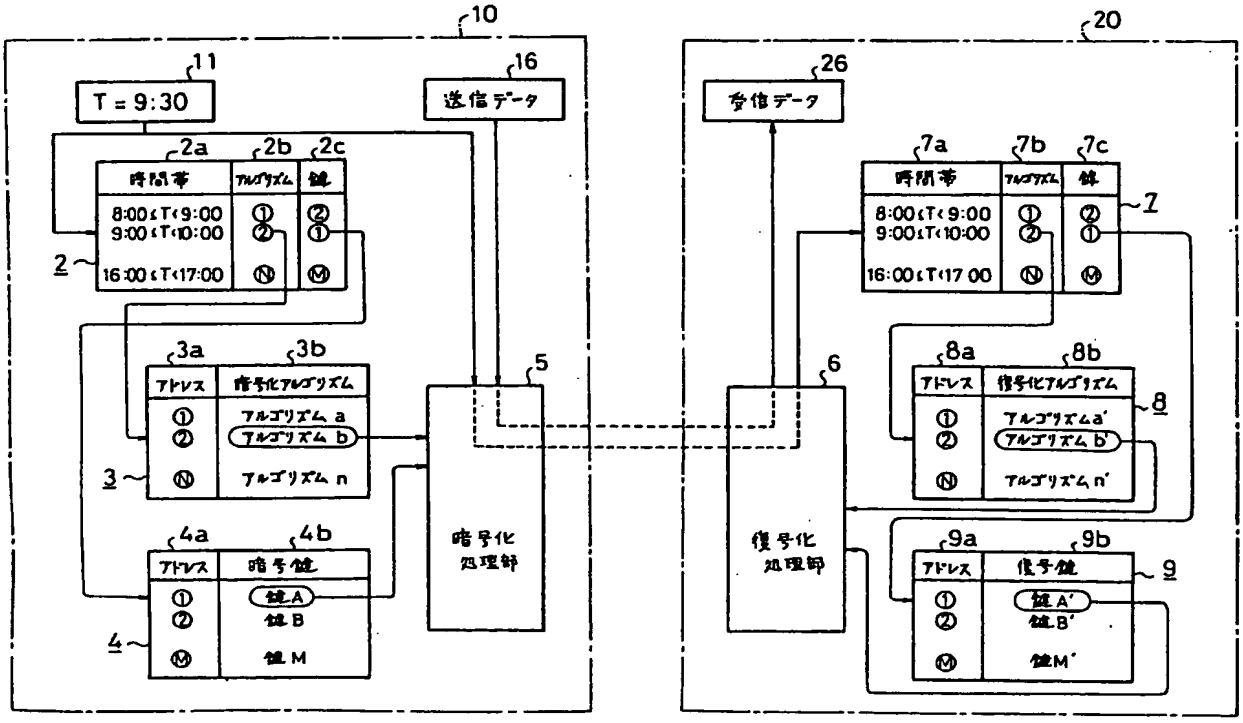
図中、10…端末機（送信側システム）、11…時計機構、12…番地生成回路、13…テーブルメモリ、14…処理用メモリ、15…処理装置、16…送信データ保持部、20…ホスト計算機（受信側システム）、22…番地生成回路、23…テーブルメモリ、24…処理用メモリ、25…処理装置、26…受信データ保持部、30…通信回線。

代理人　弁理士　秋田収喜

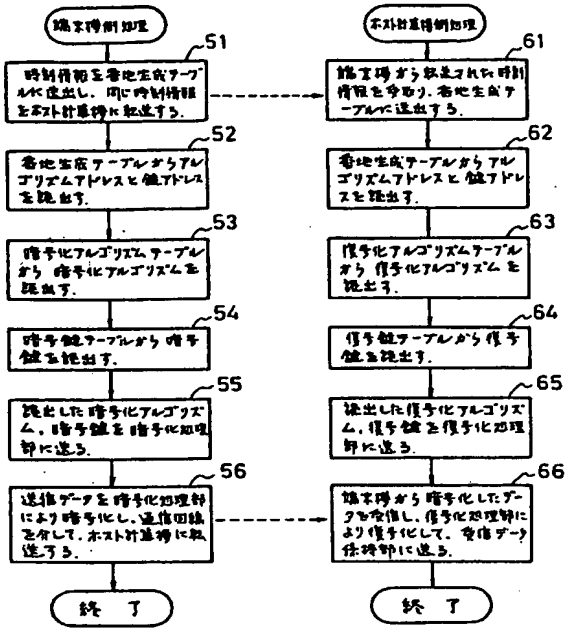
第１図



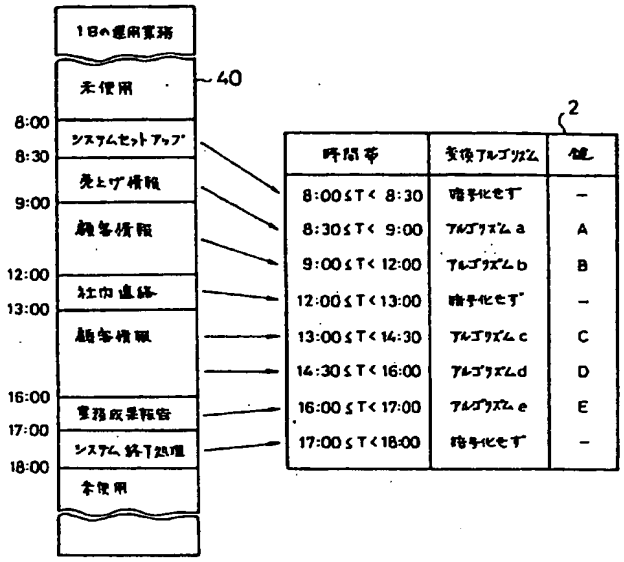
第２図



第 3 図


端末時刻処理
ホスト計算機時刻処理
時刻情報を番地生成テーブルに送出し、同に時刻情報をホスト計算機に転送する。
端末機から転送された時刻情報を受取り、番地生成テーブルに送出する。
番地生成テーブルからアルゴリズムアドレスと鍵アドレスを読出す。
番地生成テーブルからアルゴリズムアドレスと鍵アドレスを読出す。
暗号化アルゴリズムテーブルから暗号化アルゴリズムを読出す。
復号化アルゴリズムテーブルから復号化アルゴリズムを読出す。
暗号鍵テーブルから暗号鍵を読出す。
復号鍵テーブルから復号鍵を読出す。
読出した暗号化アルゴリズム、暗号鍵を暗号化処理部に送る。
読出した復号化アルゴリズム、復号鍵を復号化処理部に送る。
送信データを暗号化処理部により暗号化し、通信回線を介して、ホスト計算機に転送する。
端末機から暗号化したデータを受信し、復号化処理部により復号化して、受信データ作成部に送る。
終了
終了
51
52
53
54
55
56
61
62
63
64
65
66

第 4 図


1日の運用業務
未使用
システムセットアップ
売上げ情報
顧客情報
社内連絡
顧客情報
業務成果報告
システム終了処理
未使用
8:00
8:30
9:00
12:00
13:00
16:00
17:00
18:00
40
2
時間帯
暗号化アルゴリズム
鍵
8:00≦T< 8:30
暗号化せず
−
8:30≦T< 9:00
アルゴリズム a
A
9:00≦T< 12:00
アルゴリズム b
B
12:00≦T<13:00
暗号化せず
−
13:00≦T<14:30
アルゴリズム c
C
14:30≦T< 16:00
アルゴリズム d
D
16:00≦T< 17:00
アルゴリズム e
E
17:00≦T<18:00
暗号化せず
−